Department of Homeland Security Daily Open Source Infrastructure Report for 25 February 2009

Current Nationwide Threat Level is

ELEVATED
SIGNIFICANT RISK OF TERRORIST ATTACKS

For info click here
http://www.dhs.gov/

- According to the Virginian-Pilot, the State of Virginia for 30 years has wrongly allowed Dominion Virginia Power to discharge hot wastewater into Lake Anna from its nuclear power plant near Richmond, a circuit court judge ruled on February 20. (See item 5)
- USA Today reports that more than 100 levees in 16 states flunked maintenance inspections in the last two years and are so neglected that they could fail to stem a major flood, records from the U.S. Army Corps of Engineers show. (See item 33)

DHS Daily Open Source Infrastructure Report Fast Jump

Production Industries: Energy; Chemical; Nuclear Reactors, Materials and Waste; Defense Industrial Base; Dams

Service Industries: Banking and Finance; Transportation; Postal and Shipping; Information Technology; Communications; Commercial Facilities

Sustenance and Health: Agriculture and Food; Water; Public Health and Healthcare

Federal and State: Government Facilities; Emergency Services; National Monuments and Icons

Energy Sector

Current Electricity Sector Threat Alert Levels: Physical: ELEVATED, Cyber: ELEVATED
Scale: LOW, GUARDED, ELEVATED, HIGH, SEVERE [Source: ISAC for the Electricity Sector (ES−ISAC) − [http://www.esisac.com]

1. *February 24, Bloomberg* – (California) **BP reports fire in coke barn at California refinery.** BP Plc. reported a fire on a conveyor belt holding petroleum coke at its Carson, California, refinery. The blaze caused 500 pounds of sulfur dioxide and smoke to be released, according to a filing with the California Office of Emergency Services. The incident occurred at about 5 p.m. local time on February 23. No reason was given for the fire. The Los Angeles County Fire Department responded to the fire inside the coke barn and is the process of extinguishing it, said a second filing. The fire was under control and was not a threat to residents in the area, the Daily Breeze reported on its Web site, citing a spokesman for the refinery.
   Source:

http://www.bloomberg.com/apps/news?pid=20601072&sid=a2HwOM5e45Ns&refer=energy

2. *February 23, New York Times* – (National) **Environmentalists advance on emissions.** The Supreme Court cleared the way on February 23 for the Environmental Protection Agency to issue new regulations on emissions of mercury, lead, arsenic and other pollutants from the nation's coal-fired power plants. Environmental groups hailed the action as a final blow to the former Presidential Administration's efforts to frustrate tight regulation of the emissions, but any new current Presidential Administration rules may draw their own court challenges. The justices' action involved a suit brought by environmental organizations, Indian tribes and 14 states including New York, New Jersey, and Connecticut. The suit charged that the former Administration had acted improperly in trying to create a separate regulatory regime for the coal-fired plants rather than subjecting them to the general requirements of the Clean Air Act. The groups prevailed last year in a lower court, but the Environmental Protection Agency in the former Administration, with the support of industry groups, appealed the ruling to the Supreme Court. On February 23, the court declined to hear that appeal. Current Administration lawyers had filed papers seeking the appeal's dismissal.
Source: http://www.nytimes.com/2009/02/24/washington/24mercury.html?_r=2

3. *February 23, Reuters* – (Ohio; Michigan) **Maumee oil line in operation after leak – Sunoco.** The Maumee Ohio-to-Michigan oil pipeline which was shut on February 18 due to a leak was back on line late on February 22 as cleanup continued, Sunoco Logistics Partners LP said. Crews continued cleanup of the spill despite being hampered by icy conditions on the nearby Portage River, into which some leaking oil flowed, a Sunoco spokesman said in a news release on February 22. Restart of the pipeline minimized the risk of affecting operation of refineries served by the Maumee line. Officials had said a shutdown of less than a week was unlikely to be a problem.
Source: http://www.reuters.com/article/rbssEnergyNews/idUSN2340239420090223

4. *February 22, Cape Gazette* – (Delaware) **NRG Energy fights hostile takeover.** The attempted hostile takeover of the company that owns the Indian River power plant has raised concerns over possible environmental and human impacts of the move. Exelon Corp. of Chicago has launched a hostile takeover bid for NRG Energy, which owns the Millsboro coal-fired generating station. An Exelon Corp. spokesman said the company's plan is to sell off NRG Energy's Delaware assets, including the Indian River plant, if federal officials approve the sale. In a joint federal filing by the Delaware Public Service Commission and DNREC, the two offices said, "The potential sale of this facility to an unknown entity with unknown financial and technical capacity could prove extremely disruptive to the process and the court-mandated deadlines." Failure to comply with those orders could cause harm to human and environmental health, said the filing.
Source: http://www.capegazette.com/storiescurrent/200902/nrgtakeover20.html

[Return to top]

Chemical Industry Sector

Nothing to report

[Return to top]

Nuclear Reactors, Materials, and Waste Sector

5. *February 24, Virginian-Pilot* – (Virginia) **Judge: Nuclear plant's wastewater discharge was wrong.** The state for 30 years has wrongly allowed Dominion Virginia Power to discharge hot wastewater into Lake Anna from its nuclear power plant near Richmond, a judge ruled on February 20. Environmentalists hailed the decision by a Richmond circuit court judge. They said it should lead to first-ever regulations of atomic wastewater and cool parts of Lake Anna, a central Virginia landmark known to eclipse 100 degrees on summer days. "This is huge," said a science director for the Blue Ridge Environmental Defense League. "We and lakeside residents have long believed that Dominion is guilty of thermal pollution." Such pollution, he said, threatens human health, property values and aquatic life. The court ruling also could complicate a billion-dollar proposal from Dominion to expand its North Anna nuclear power plant by building a third reactor on Lake Anna in Louisa County. While Dominion has recommended an air-cooling system for the new reactor, the project still would influence lake levels and temperatures, said the president of Friends of Lake Anna, a conservation group. The judge turned this interpretation on its ear. The judge instructed the State Water Control Board to draft a new discharge permit for the nuclear station so that the lake never exceeds 89.6 degrees, said a Richmond attorney representing the environmentalists.
   Source: http://hamptonroads.com/2009/02/judge-nuclear-plants-wastewater-discharge-was-wrong

6. *February 23, U.S. Nuclear Regulatory Commission* – (Nebraska) **NRC conducting special inspection at Cooper Nuclear Station.** The U.S. Nuclear Regulatory Commission is conducting a special inspection at the Cooper Nuclear Station in response to the failure of a pipe that supplies lubricating oil to an emergency diesel generator. On January 27, during a monthly surveillance test of the diesel, the pipe began leaking oil. The licensee believes the leak was caused by a vibration induced failure. The diesel generators are used to supply power to plant safety systems in the event of a loss of off-site power during emergencies. A year ago, a leak was found in a similar pipe supplying oil to a second emergency diesel generator. The licensee replaced pipes on both diesel generators. "Based on this most recent leak, and the similarity of the problems, we have questions about the effectiveness of the licensee's corrective actions and we want to take a closer look at this matter," said the region 4 administrator. A four-member team of NRC specialists will review the circumstances related to the event, the licensee's root cause evaluation and determine whether appropriate corrective actions were taken. The team includes three reactor inspectors from the NRC's region 4 office in Arlington, Texas, and a member of the Office of Nuclear Regulatory Research from NRC Headquarters in Rockville, Maryland. The inspection began today and is expected to take several days. The team will write a report about 30–45 days after completion of the inspection.
   Source: http://www.nrc.gov/reading-rm/doc-collections/news/2009/09-002.iv.html

[Return to top]

Defense Industrial Base Sector

7. *February 23, NASASpaceFlight.com* – (National) **Orbital's Taurus XL fails during Orbiting Carbon Observatory spacecraft launch.** Orbital Science's Taurus XL rocket lifted-off from Space Launch Complex 576-E at Vandenberg Air Force Base, California, carrying the Orbiting Carbon Observatory (OCO) Monday morning. However, the mission was deemed a failure during or slightly after third stage flight, after it was noted the fairing failed to separate as required. "OCO did not achieve orbit successfully," noted Vandenberg's public affairs officer in an anomaly update. A later update confirmed the vehicle had failed to make orbit due to lack of delta V that would have been gained by the loss of the heavy fairing; the spacecraft eventually splashed down near Antarctica. Taurus' next mission, with the GLORY satellite, will remain on hold, pending the conclusion of the investigation.
Source: http://www.nasaspaceflight.com/2009/02/orbitals-taurus-xl-launch-orbiting-carbon-observatory/
See also: http://www.cnn.com/2009/TECH/space/02/24/nasa.launch/index.html

[Return to top]

Banking and Finance Sector

8. *February 24, Quincy Patriot Ledger* – (Massachusetts) **'Phishing' scam targets South Coastal Bank patrons.** An apparent telephone scam attempts to obtain South Coastal Bank customers' account information. Several Rockland residents, including a bank employee, received the calls, the bank reported on February 23. The recorded message claimed to be from South Coastal Bank. The message said their ATM card had been deactivated and asked them to enter their account information to reactivate the card. The president and CEO of Rockland-based bank said the organization does not know of any customers who gave out their account information. The bank never asks customers for confidential information over the phone, he said.
Source: http://www.patriotledger.com/business/x1739334314/-Phishing-scam-targets-South-Coastal-Bank-patrons

9. *February 23, Bloomberg* – (National) **U.S. pledges new capital for banks as stress tests to begin.** U.S. financial regulators pledged to inject additional funds into the nation's major banks to prevent their collapse and will this week begin examinations to determine if they have enough capital. "The government will ensure that banks have the capital and liquidity they need to provide the credit necessary to restore economic growth," the Treasury and other regulators said in a joint statement in Washington on February 23. "The U.S. government stands firmly behind the banking system during this period of financial strain." Banks that need additional funds after the so-called stress tests that cannot raise the money from private investors will be able to tap additional taxpayer money, the regulators said. Government funds would be in the form of "mandatory convertible preferred shares" that would be exchanged into common equity

"only as needed." Stakes that the Treasury has already bought in lenders, such as Citigroup Inc. and Bank of America Corp., will also be eligible to be changed to convertible preferred shares. The new funds are designed to provide a "temporary" buffer for firms against increased losses during the crisis. Supervisors will start the stress tests on February 25 to assess whether banks have enough capital to withstand "a more challenging economic environment."
Source:
http://www.bloomberg.com/apps/news?pid=20601087&sid=anQdy0Qb32lc&refer=home

10. *February 23, WBNG 12 Binghamton* – (New York) **Text message scam can wipe out money in minutes.** BCT Federal Credit Union in Binghamton opened this morning to some worried customers. The customers received text messages on their cell phones, asking for personal banking information. One individual received two messages saying her debit card had been deactivated and she needed to call a number to reactivate it. "I looked in the phone book actually for the GHS phone number because I knew the phone number they had on here probably wasn't right and told them I didn't have an account with them and I got this text message...and they told me it was a scam," said the woman. BCT said those who provided their personal information instantly had their bank accounts wiped out. A representative of the credit union guesses about 100 peoples' accounts were wiped out. Individuals who received the message said they had received texts claiming they are GHS, BCT and Empower Federal Credit Unions. These institutions said they would never send anyone a text message asking for personal information.
Source: http://www.wbng.com/news/local/40121632.html

11. *February 23, Shelby Star* – (North Carolina) **Scam targets area texters.** A suspicious text message has been sent to Shelby-area cell phone customers claiming that their account has been closed and instructing them to call a phone number. One individual says he received the text message from "jim@foundationmortgage.com," and called the phone number. When he did, a recording, allegedly from Fleet Bank, alerted him that there was suspicious activity to his bank account. But this individual did not have an account at Fleet Bank and when the recording instructed him that they needed his credit card number, he hung up. In December 2008, the Star reported a similar scam popped up in West Virginia. Vague messages implore the recipient to reactivate their bankcard. Account information required, of course. At that time, police said they had yet to hear reports of it occurring in Cleveland County. The Cleveland County Sheriff's Office said this scam mirrors several scams that are targeting locals. A captain with the sheriff's office said residents should never give out their credit card information, personal information or bank account information to unknown people.
Source:
http://www.shelbystar.com/news/greene_37201___article.html/message_information.html

12. *February 23, SearchFinancialSecurity.com* – (National) **Credit unions confirm new processor credit card breach.** A payment processor is in the process of identifying the

extent of damage caused by a malicious program discovered in its systems exposing credit and debit card numbers. MasterCard and Visa are issuing information to banks and credit unions about credit and debit card accounts that were exposed in the data security breach of a second payment processor in less than two months. The Pennsylvania Credit Union Association and the Tuscaloosa, Alabama VA Federal Credit Union posted messages on their Web sites explaining that a breach investigation is ongoing. Both Visa and MasterCard are declining to name the processor while a forensics team investigates the breach. Investigators are also trying to find a link between the latest breach and the recently announced Heartland Payment Systems breach, a credit union official said under condition of anonymity. Visa began releasing information to banks and credit unions about affected accounts on February 9. A vulnerability left potentially thousands of credit and debit card numbers exposed for a period between February 2008 through January 2009, according to an alert issued by the Tuscaloosa VA Federal Credit Union. "We have not been notified that any of our cardholders have fraudulent activity due to this compromise," the message stated. "While it has been confirmed that malicious software was placed on the processor's platform, there is no forensic evidence that accounts were viewed or taken by the hackers." Credit union officials said it appears the breach is not as serious as the Heartland breach.
Source:
http://searchfinancialsecurity.techtarget.com/news/article/0,289142,sid185_gci1348856,00.html

[Return to top]

Transportation Sector

13. *February 24, CNN* – (Washington) **Pilots landing at Seattle-Tacoma airport report lasers.** Pilots on 12 jetliners landing at Seattle-Tacoma International Airport on February 22 reported that someone was shining a green laser light into their cockpits, bringing renewed attention to a problem that has plagued pilots since the introduction of cheap laser pointers several years ago. The planes, targeted during a 20-minute period, all landed safely. But the incident led to pilots simultaneously trying to avoid being temporarily blinded by the light while trying to help authorities pinpoint its source, believed to be about a mile north of the airport. Air traffic controllers continuously cautioned pilots about the light during the episode. Laser attacks on aircraft have increased in recent years, according to the Federal Aviation Administration. There have been 148 incidents this year, an FAA spokeswoman said.
Source:
http://www.cnn.com/2009/US/02/23/washington.plane.lasers/index.html?iref=newssearch

14. *February 24, Associated Press* – (Connecticut) **Airline ordered to pay $400,000 to 'whistleblower.'** Federal authorities have ordered a Connecticut-based cargo airline to pay more than $400,000 to a flight crew member who was fired after raising safety concerns. Occupational Safety and Health Administration officials said this week that they have ordered Southern Air Inc. to compensate the employee for lost wages, back

pay, damages and legal fees. OSHA officials say the crew member was fired by Norwalk-based Southern Air in April 2008 after complaining that workers lacked adequate rest breaks and were being forced to work more hours than federal rules allow. The employee filed a whistleblower complaint with OSHA. Messages seeking comment were left Tuesday with Southern Air executives.
Source: http://www.courant.com/news/local/hcu-ap-airline-0224,0,3793007.story

15. *February 23, WJLA 7 Washington, D.C.* – (Louisiana) **Possible bird strike eyed in chopper crash.** Investigators have found evidence that a bird may have struck a helicopter before it crashed into a Louisiana swamp last month, killing eight people, the National Transportation Safety Board said Monday. The NTSB has not identified the cause of the deadly crash near Morgan City on January 4, but said tests on the wreckage of the Sikorsky S-76C found microscopic bird remains of a "hawk variety" on the pilot's side of the chopper's windscreen. Investigators also found parts of feathers under a windscreen seal and in an engine, the NTSB said in a press release. A Department of Agriculture bird specialist examined the wreckage last month and did not see any visible evidence of a bird strike, but tests at the Smithsonian Institution Feather Identification Lab revealed the microscopic bird remains. A DNA test showed it was a variety of hawk, according to the NTSB statement. The NTSB said Monday it will continue to analyze information from the chopper's cockpit voice and flight data recorders. The investigation also will include "research into the potential scenarios that could cause the loss of engine torque and electrical anomalies noted on the flight recorders," the release said.
Source: http://www.wjla.com/news/stories/0209/597660.html?ref=rs

16. *February 22, Associated Press* – (Oklahoma) **Concrete shakes loose from Okla. bridges.** In the four years since a Texas woman was killed when a piece of concrete fell from an interstate bridge and crashed through her windshield, more than two dozen other people have filed similar claims against the state. Although no deaths were reported, information provided to the Associated Press under an open records request shows 26 people have filed claims against the state involving falling concrete since the fatal accident in June 2004. In all but two of the cases, the state denied the claims, usually saying the claimant failed to show the state was actually negligent. Injuries were claimed in two cases. Transportation officials say they are required to inspect bridges every two years, and if they do that and find no indication of loose concrete, they are not liable for damages if a chunk of that bridge should fall. Federal Highway Administration data for 2008 show that 5,566 or 24 percent of Oklahoma's 23,587 bridges are structurally deficient, second only to Pennsylvania.
Source: http://www.kswo.com/Global/story.asp?S=9886209

[Return to top]

Postal and Shipping Sector

17. *February 24, WCPO 9 Cincinnati* – (Ohio) **Suspicious package found at post office.** There were some tense moments at a Cincinnati post office on February 24 after a worker discovered a suspicious package in the building. A worker at the U.S. post office

in Queensgate called 911 to report finding the suspicious substance just after midnight. According to emergency radio reports, the employee told crews the sandy substance caused her hand to turn red after touching it. An expert was called to the scene to test the substance, and officials later determined it was not hazardous.
Source: http://www.wcpo.com/news/local/story/Suspicious-Package-Found-At-Post-Office/4v_rnIP3hE6rY_cODItBGQ.cspx

[Return to top]

Agriculture and Food Sector

18. *February 23, Associated Press* – (North Dakota) **ND mulls tougher regs of farm chemical application.** Water resource advocates have lost a round in the North Dakota Legislature but they are not giving up the push for more stringent rules on the use of irrigation systems to apply farm chemicals. A bill defeated in the Senate on a 22-24 vote would have set up a permit system for chemigation through the Agriculture Department. The Agriculture Department's lead farm chemical regulator said the important aspect of such a system would not be the money it would bring in, but the fact that it would set up a registry to let regulators know where chemigation outfits are located. Right now, he said, "there is no good data source for us to go to, to find out exactly where chemigating is taking place." Farmers say applying fertilizer and pesticides through irrigation systems can be easier and cheaper than other methods. Opponents say the practice can contaminate groundwater if the chemical tanks leak or spill. A North Dakota farmer who wants to set up a chemigation system must follow design rules and install a device that prevents the backflow of chemicals into the water well supplying the irrigation system. The bill defeated in the Senate would have required the agriculture commissioner to study new rules and report back to the Legislative Council — the Legislature's research arm — by July 2010.
Source: http://www.forbes.com/feeds/ap/2009/02/23/ap6083357.html

[Return to top]

Water Sector

19. *February 24, Associated Press* – (Maryland) **Untreated wastewater gushes into wooded area.** A blocked sewer line sent an overflow of 10,700 gallons of untreated wastewater into a wooded area in Laurel, Maryland, say Washington D.C. Suburban Sanitary Commission (WSSC) officials. The overflow near the 800 block of White Way in Laurel on the evening of February 22 sent wastewater into a storm drain for a tributary of the Patuxent River. A WSSC spokesman says when sanitation workers discovered the problem the sewage was flowing at a rate of 50 gallons per minute. Workers cleared the line clogged by grease and rags and have posted signs warning residents to avoid the area around the tributary during the next 30 days.
Source: http://www.wtop.com/?nid=25&sid=1608995

20. *February 24, Pottstown Mercury* – (Pennsylvania) **DEP study assessing nuclear waste levels in Schuylkill River.** A facility that cleans the uniforms of nuclear industry

employees, including those at the Limerick Generating Station, is monitoring the buildup of low-level radioactive material in the Schuylkill River. UniTech Services Group Inc. has discharged treated wastewater into the Schuylkill River since 2004, in accordance with safety standards set by the Pennsylvania Department of Environmental Protection (DEP) and the Nuclear Regulatory Commission. On February 20, DEP issued a news release updating the public on its "field investigation," which began last summer in an effort to learn more about the possible cumulative effects of such discharges on both the river and its ecosystem. "At no time did UniTech exceed its permitted discharge limits for radionuclides," the regional DEP director stated. "However, based on our analysis of sludge that settled out at the Royersford's wastewater treatment plant, we now know that low-level radioactive material in liquid effluents can become concentrated over time." In December, DEP extended the investigation to the nearest downstream water supplier in Phoenixville. No radionuclides have been detected above state and federal drinking water standards to date, the agency stated. "Recreational contact" with the Schuylkill River, including the consumption of fish, poses no risk to human health, the agency stated. Still, DEP described these results as preliminary and said further study is needed.
Source: http://www.pottsmerc.com/articles/2009/02/24/news/srv0000004749525.txt

[Return to top]

Public Health and Healthcare Sector

21. *February 24, Reuters* – (International) **Bird flu vaccine production still lags – study.** Drug companies have increased their capacity to make bird flu vaccines by 300 percent in the past two years but will still need four years to meet global demand in the event of a pandemic, a study said on Tuesday. It also said doses of vaccine tailored to the actual strain of pandemic influenza that emerges will not be available until four months after that strain is identified. "We found that considerable progress has been made to enhance the production capacity of pandemic influenza vaccine," a partner at consulting firm Oliver Wyman, which conducted the study, said in a statement. "While capacity still falls short of global need during a pandemic, the surplus capacity during the inter-pandemic period creates opportunities for preparedness efforts," he said. Manufacturers hunting for the best vaccines to stop the deadly disease face a race against the clock if the H5N1 strain of influenza now circulating in birds mutates and starts spreading easily among humans, as many researchers fear.
Source: http://uk.reuters.com/article/rbssHealthcareNews/idUKLO69365620090224

22. *February 23, HealthDay News* – (National) **White House to send $15 billion to states for Medicaid.** The Presidential Administration intends to distribute $15 billion within two days to help cash-strapped states cope with Medicaid payments to the poor. The $15 billion is part of the newly passed $787 billion economic stimulus program, the U.S. President told governors during a White House meeting Monday, the Associated Press reported. Medicaid is underwritten jointly by states and the Federal Government.
Source: http://www.healthday.com/Article.asp?AID=624403

[Return to top]

Government Facilities Sector

23. *February 24, CNET News* – (National) **Borg-like cybots may patrol government networks.** The Oak Ridge National Laboratory has created software that uses colonies of borg-like cyberrobots it says will help government agencies detect and fend off attacks on the nation's computer network infrastructure. The Ubiquitous Network Transient Autonomous Mission Entities (Untame) differs from traditional security software agents in that its cybot "entities" form collectives that are mutually aware of the condition and activities of other bots in their colony. When these cybots detect network intruders, they communicate with one another, preventing cybercrooks from creating and using a diversion in one spot within the network to then break through in another. "The cybots are an inherent part of Untame's software, designed to do cybersecurity," said a team leader from the lab's Computational Sciences and Engineering Division, said in an interview with the Daily Beacon. "Most enterprises have intrusion detection centers set up in key spots, but they don't communicate with each other. But a cybot is intended to work with other cybots, continue their mission, or regenerate when necessary so they can pick up where one left off." The U.S. Department of Energy commissioned the software, in response to criticism from Congress (PDF) over security lapses. It hopes for an "intelligent, self-healing, intrusion detection and prevention system" capable of real-time response and defense, one that can learn to avoid false positives and relieve human operators from sloughing through low-level alerts.
Source: http://news.cnet.com/8301-13639_3-10169564-42.html

24. *February 23, Computerworld* – (Florida) **Three months, three breaches at Florida University.** For the second time in three months, the University of Florida in Gainesville has acknowledged a major data breach, and a statement posted on the university's Web site indicates that there was a third, less public, breach discovered by the school during the same period. On February 19 the university disclosed that a server installed more than a decade ago to support a free e-mail service and to give faculty a way to host online course materials had been breached, exposing personal data on 97,200 students, faculty and staff that used it between 1996 and 2009. The server intrusion was discovered in January during a routine systems review by a university IT staffer. It is not clear when the system may have been compromised or for how long an intruder had access to the data in it, said a university spokeswoman. The compromised information included Social Security Numbers and the full names of staff, students and faculty. A forensic investigation of the breach has shown that the attacker used an IP address that appears to have been located in Antigua and Barbuda, she added. A majority of those affected by the breach are being notified about it, but the university does not have contact information for about 5,000 people and has been unable to inform them, she said.
Source: http://www.networkworld.com/news/2009/022309-three-months-three-breaches-at.html

25. *February 23, Computerworld* – (National) **Hackers shut down travel site for federal workers.** A travel reservations Web site used by several federal agencies was hit during

the early part of February by hackers, who shunted unsuspecting users off to a malicious domain. The site, GovTrip.com, remained unavailable during the week of February 16-20. According to an e-mail sent to federal workers by the General Services Administration, the site was breached before February 11. The agency did not say when the site will be back online. A GSA spokesman last week said that "the incident was quickly identified." He declined to disclose details, citing an ongoing investigation into the hack. The GSA e-mail, however, said that the hackers modified GovTrip.com to redirect users to a rogue URL that launched attack code into their systems. The spokesman did say that no user information is believed to have been compromised. The site is operated by Northrop Grumman Corp. GovTrip is used by several U.S. government agencies, including the Environmental Protection Agency and the Energy, Interior, Transportation, Treasury, and Health and Human Services departments. The spokesman said that the affected departments, the GSA and Northrop Grumman are working "to identify short-term and long-term measures to find the source of the incident and to prevent such an incident from recurring."
Source: http://www.computerworld.com/action/article.do?command=viewArticleBasic&articleId=334522&intsrc=news_ts_head

26. *February 23, Virginian-Pilot* – (Virginia) **Suspicious package found at Portsmouth Naval Medical Center.** A parking garage at Portsmouth Naval Medical Center was closed and K-9 and explosive ordinance disposal units called in to investigate a suspicious package, a spokeswoman said. The suspicious package was discovered at 4:46 p.m. on February 23, said a naval spokesman. Emergency responders also checked the parking garage for any other suspicious packages. The parking garage was cleared at about 9:10 p.m. when investigators determined the package was someone's personal belongings, said the naval spokesman.
Source: http://hamptonroads.com/2009/02/suspicious-package-found-naval-medical-center-portsmouth

[Return to top]

Emergency Services Sector

27. *February 24, Dallas Morning News* – (Texas) **Dallas-Fort Worth area to have new warning guidelines for storm emergencies.** North Texas emergency officials announced new guidelines on Monday for outdoor warning systems to establish a standard for notifying residents of severe weather and other potentially catastrophic events across the region. The North Central Texas Council of Governments formally unveiled the recommendations to kick off severe weather awareness week. Outdoor warning systems are typically referred to as tornado sirens but can be activated for other reasons. The director of emergency preparedness for the council said most government agencies in Dallas, Tarrant, Collin and Denton counties have agreed to adopt the guidelines. Each city also has discretion to use a warning system for any other reason.
Source: http://www.dallasnews.com/sharedcontent/dws/news/localnews/stories/022409dnmetstormguidelines.4c2f56d.html

28. *February 23, WRTV 6 Indianapolis* – (Indiana) **911 calls going to wrong county in border zones.** Residents who live in an area that borders three counties are worried that they might not be properly routed to the correct 911 center in the event of an emergency. Residents of Heartland Crossing, which is in Morgan County but closely borders Hendricks and Marion Counties have reason for concern, 6 News reported. A resident called 911 from his cell phone on February 16 to report a fire. The call went to a tower in Marion County, which improperly sent the call to Indianapolis, costing several minutes of response time. Response from a fire department less than a mile away from his home was delayed for several minutes before the correct dispatchers received the call.
Source: http://www.theindychannel.com/news/18778798/detail.html

[Return to top]

Information Technology

29. *February 24, IDG News Service* – (International) **Attackers targeting unpatched vulnerability in Excel 2007.** Microsoft's Excel spreadsheet program has a 0-day vulnerability that attackers are exploiting on the Internet, according to security vendor Symantec. A 0-day vulnerability is one that does not have a patch and is actively being used to attack computers when it is publicly revealed. The problem affects Excel 2007 and the same version of that program with Service Pack 1, according to an advisory on SecurityFocus, a Web site that tracks software flaws. Other versions of Excel may also be affected, it said. The program's vulnerability can be exploited if a user opens a maliciously-crafted Excel file. Then, a hacker could run unauthorized code. Symantec has detected that the exploit can leave a Trojan horse on the infected system, which it calls "Trojan.Mdropper.AC." That Trojan, which works on PCs running the Vista and XP operating systems, is capable of downloading other malware to the computer. Microsoft said it is only aware of "limited and targeted attacks" and that it would release more information on February 24. Hackers have increasingly sought to find vulnerabilities in applications as Microsoft has spent much effort into making its Vista OS more secure.
Source: http://www.networkworld.com/news/2009/022409-attackers-targeting-unpatched-vulnerability-in.html

30. *February 23, ComputerWeekly* – (National) **U.S. publishes National Cybersecurity Strategy critical security controls.** The U.S. has published a draft list of critical security controls to protect key national information systems from cyber attack. The move is the first step towards creating a comprehensive U.S. national cyber security strategy as recommended by a special advisory commission. The Center for Strategic and International Studies (CSIS), a Washington-based think tank, set up the commission in August 2007 after a series of cyber attacks on critical information systems. The CSIS Commission on Cybersecurity is tasked with advising the U.S. President's government on how to protect federal information systems and critical infrastructure from attack. The draft controls, known as the Consensus Audit Guidelines, are based on input from 10 federal agencies, Mitre Corporation, Sans Institute, and two penetration testing and

forensics firms. The Consensus Audit Guidelines (CAG) project was started in 2008 after data losses by leading U.S. defense industry firms. The goal was to draw up a risk-based standard to counter all known types of cyber attack. "This is the best example of risk-based security I have ever seen," said the director of research at the Sans Institute. Source: http://www.computerweekly.com/Articles/2009/02/23/234969/us-publishes-national-cybersecurity-strategy-critical-security.htm

31. *February 23, Computerworld* – (International) **Adobe flaw has been used in attacks since early January.** A dangerous and unpatched vulnerability in Adobe Systems Inc.'s PDF-reading software has been around a lot longer than previously realized. The Adobe Reader flaw, which was first reported recently, has caused concern because the bug is easy to exploit and Adobe is not expected to patch it for several weeks. A vulnerability researcher at intrusion-prevention vendor Sourcefire Inc. posted a patch for the flaw on February 22. But the unsupported patch applies only to the Windows version of Adobe Reader 9.0 and comes with no guarantees that it will actually work. Security researchers at Symantec Corp. told Adobe about the flaw, which also affects the vendor's Acrobat software, on February 12. But on February 23, Sourcefire said an analysis of its malware database showed that attackers have been exploiting the flaw for more than six weeks. Sourcefire has found samples of exploit code dating back to January 9, said the company's senior director of vulnerability research. To date, the flaw has been used in small-scale attacks targeted against specific individuals, according to security researchers. Symantec, for example, said it has tracked only 100 attacks thus far. But that number has been increasing since exploit code for the flaw, which affects both Windows and Macintosh users, was made public.
Source:
http://www.computerworld.com/action/article.do?command=viewArticleBasic&taxonomyId=18&articleId=9128479&intsrc=hm_topic

Internet Alert Dashboard

To report cyber infrastructure incidents or to request information, please contact US−CERT at soc@us−cert.gov or visit their Website: http://www.us−cert.gov.

Information on IT information sharing and analysis can be found at the IT ISAC (Information Sharing and Analysis Center) Website: https://www.it−isac.org/.

[Return to top]

Communications Sector

Nothing to report

[Return to top]

Commercial Facilities Sector

32. *February 23, Associated Press* – (National) **Meth makers leave behind a toxic trail at motels.** Methamphetamine "cooks" are secretly converting hundreds of motel and hotel

rooms into covert drug labs — leaving behind a toxic mess for unsuspecting customers and housekeeping crews. The dangerous contaminants can lurk on countertops, carpets and bathtubs, and chemical odors that might be a warning clue to those who follow can be masked by tobacco smoke and other scents. Motels can be an attractive alternative for drug makers seeking to avoid a police raid on their own homes. U.S. Drug Enforcement Administration records obtained by the Associated Press show that states reported finding evidence of drug-making in 1,789 motel and hotel rooms in the past five years — and that is just those the authorities found. The toxins can linger for days if meth lab hygienists wearing hazmat suits do not clean living areas. The cleanups cost anywhere from $2,000 to $20,000. Even short-term exposure to vapors and residue where the drug is smoked or cooked can cause eye and skin irritation, vomiting, rashes, asthma problems and other respiratory issues. The volatile labs can be set up in less than four hours inside a hotel or motel room, according to the American Hotel and Lodging Association. Methods vary for making the drug, but the equipment can be simple enough to fit in a single backpack: a large soft drink bottle with some rubber tubing, duct tape, batteries, refrigerant packs and a decongestant that contains ephedrine or pseudoephedrine.
Source: http://www.google.com/hostednews/ap/article/ALeqM5hURpCyvmobWZxgcVbt83u2oHLvUwD96HCFBG0

[Return to top]

National Monuments & Icons Sector

Nothing to report

[Return to top]

Dams Sector

33. *February 24, USA Today* – (National) **Army Corps cracks down on flunking levees.** More than 100 levees in 16 states flunked maintenance inspections in the last two years and are so neglected that they could fail to stem a major flood, records from the U.S. Army Corps of Engineers show. The 114 levees received “unacceptable” maintenance ratings in Corps inspections, meaning their deficiencies are so severe that it can be “reasonably foreseen” that they will not perform properly in a major flood, according to the records, which were requested by USA Today. As a result, the Corps is advising state and local levee authorities that the levees no longer qualify for federal rehabilitation aid if damaged by floodwaters. People who rely on the levees should “be aware that there is reason for concern,” says the head of the Corps’ levee safety program.
Source: http://www.usatoday.com/news/nation/2009-02-23-levees_N.htm

34. *February 23, KAPP 35 Yakima* – (Washington) **High hazard dams must be fixed.** The Department of Ecology is ordering immediate repairs for eight private dams in Yakima County, Washington. These dams are considered highly hazardous. The fruit companies

that own them must fix them before they can be filled for frost control. Before they can be used, the dams must be able to survive a once-in-25-years-flood. Within the next two years, the dams must be up to the 100-year level. The high hazard classification indicates there are between 7 and 300 people at risk if the dam fails. The owners are looking at spending thousands of dollars to get up to standards.
Source: http://www.kapptv.com/news/?sect_rank=1&section_id=22&story_id=12551

35. *February 23, Contra Costa Times* – (California) **Report: Enlarging Los Vaqueros Reservoir could solve water woes.** Enlarging an eastern Contra Costa reservoir to nearly three times its current size could alleviate some of the delta's environmental problems and stabilize water supplies in the Bay Area, according to an environmental report released on February 23. The report, by the Contra Costa Water District and the U.S. Bureau of Reclamation, says if other Bay Area water agencies hook into Los Vaqueros Reservoir, fewer fish will be killed at massive pumping stations near Tracy that are run by the state and federal governments. The protective intake screens at the reservoir near Livermore, which was completed in 1997, are much less destructive to fish than the larger Delta pumping stations, which date to the 1940s. And beyond that, a larger reservoir could also stabilize water supplies in the Bay Area during droughts, the report said. Despite recent rains, California's biggest reservoirs are only about half as full as normal for this time of year and the snowfall in the northern Sierra, which is key for the state's water supply, remains below average.
Source: http://www.mercurynews.com/breakingnews/ci_11769517

[Return to top]

DHS Daily Open Source Infrastructure Report Contact Information

DHS Daily Open Source Infrastructure Reports − The DHS Daily Open Source Infrastructure Report is a daily [Monday through Friday] summary of open−source published information concerning significant critical infrastructure issues. The DHS Daily Open Source Infrastructure Report is archived for ten days on the Department of Homeland Security Website: http://www.dhs.gov/iaipdailyreport

DHS Daily Open Source Infrastructure Report Contact Information

Content and Suggestions:	Send mail to NICCReports@dhs.gov or contact the DHS Daily Report Team at (202) 312-3421
Subscribe to the Distribution List:	Visit the DHS Daily Open Source Infrastructure Report and follow instructions to Get e-mail updates when this information changes.
Removal from Distribution List:	Send mail to support@govdelivery.com.

Contact DHS

To report physical infrastructure incidents or to request information, please contact the National Infrastructure Coordinating Center at nicc@dhs.gov or (202) 282−9201.
To report cyber infrastructure incidents or to request information, please contact US−CERT at soc@us−cert.gov or visit their Web page at www.us−cert.gov.

Department of Homeland Security Disclaimer